Part 3. Human-Centred Security

Tia C

1. Human-Centred Risks

Phishing can be carried out by attackers in both a targeted attack or flooding attack, where phishing emails and texts are sent to multiple companies. These attacks can allow attackers to install malware, steal passwords and gain a foothold within the company's network(s). Employees within a company tend to be on the front-line of these attacks, meaning they are responsible for identifying and reporting phishing attempts (NCSC, 2018).

Phishing is a social based security risk, relying on human nature to be successful. This is evidenced by a literature review from Cardiff Metropolitan University in which the anatomy of phishing attacks is analysed. Authority cues and urgency are utilised by attackers in attempts to socially engineer victims to click the links (2021). This is explored further by Sharma and Bashir's study which analysed how phishing emails use emotional triggers to lure victims into clicking. The study found that attackers aimed to exploit feelings of "fear, anticipation and trust" as well as engaging a victim's curiosity (2020).

Phishing attacks risen during the pandemic due to lockdowns and the need to work from home. A study by Georgiadou et al (2021) found cyber security was affected by employees working from home (hereinafter, WFH). Over half of employees surveyed did not have security guidelines from their employers, with "experienced technology users reporting phishing…". This is supported by a survey carried out by the government with 83% out of 654 businesses saying they identified phishing attacks in their business (GOV.UK, 2021). They were particularly worried due to employees WFH, that the employees and business would be more susceptible to cyber risks as they cannot be monitored as they would in an office. These studies show that phishing is a serious risk to businesses, with criminals taking advantage of employees working from home and the lack of security protocols in place.

A literature review looking into human factors within phishing attacks identified that lack of knowledge, resources and awareness were the three main vulnerable factors exploited by phishing attempts (Desolda et.al, 2021). This also supports the previous research by Georgiadou et.al and the government, that lack of guidance and resources affects employee's susceptibility to phishing attempts. This is further evidenced in Hadlington's study into human factors within cybersecurity (2017), noting that the more impulsive a person was – the less likely they were to recognise a phishing attempt. The study also found that the majority of participants believed management was responsible for enforcing good cybersecurity in a company. This emphasises the need for companies to ensure that employees understand their role within the company regarding cybersecurity.

With these factors in mind, countermeasures to tackle phishing need to consider human factors, emotions, and behaviours.

2. Human-Centred Recommendations

A literature review by Jampen et al identified that educating users through anti-phishing training such as getting employees to identify phishing emails and educate about phishing and how it works is effective. However, they found that such training is not a one-size fits all measure and needs to be adjusted to ages and technological ability (2020). When running phishing tests, the number of links clicked, sensitive data entered, and number of emails reported should be gathered and evaluated. Employees who click links and enter usernames and passwords should receive more personal training, whilst encouraging employees who reported the emails (Dashlane Blog, 2020). As well as training, employees should be given guidance regarding WFH and cybersecurity as highlighted by Georgiadou et al.

Gamification and applied games may also be a suitable way to train employees about cybersecurity and phishing. A role-playing game was created with the main goal of educating players about phishing in an engaging way. The game provides feedback each time the player makes a choice and is realistic, for example if the player clicks a malicious link – their mistake will be highlighted and explained to them. It also encourages the player to ask for help if they are unsure, which should be common practice in the workplace (Wen et al., 2019).

One software measure that should be implemented to protect employees is Microsoft 365's anti-phishing protection. These features include authentication checks, and spoof checks to prevent malicious emails being sent to employees. Microsoft Defender also allows for administrators to perform anti-phishing campaigns, which means the company do not need to pay for specialist software or a company to perform these campaigns and training (Microsoft 365, 2022).

As employees have already received phishing emails, the software and training recommendations should be applied as soon as possible. If the business grows in size, these recommendations should be re-evaluated. For example, professional phishing simulations may be more suitable for a medium to large size business – however, Microsoft Defender is more than suitable for the size of small business that ScottishGlen currently is.

3. Authentication Mechanisms

Authentication mechanisms can use three different factors, they are *something you **know,*** *something you **have*** and *something you **are.*** However, the effectiveness of each factor will be dependent on the context they are being used in. A review of authentication methods carried out by Lal et.al suggests that passwords, RFID smart cards, and biometric authentication are viable authentication methods, and that biometric authentication can provide the most secure form of authentication (2016). These authentication methods can be found in real world situations; however, Rui and Yan argue that biometric authentication does not provide satisfactory privacy protection for the user and that biometric authentication can be spoofed with little effort. They also note that biometric authentication requires a large amount of processing power to implement (2018). This means that biometric authentication may not be a suitable option for ScottishGlen due to the processing power required. Employees may not be comfortable with the lack of privacy protection surrounding biometric authentication.

Passwords represent the something you **know** authentication factor and have been used for many years. However, they are very susceptible to attacks such as brute-forcing and password cracking. They are also inaccessible for people with learning difficulties such as dyslexia as identified by research carried out by Renaud, Johnson and Ophoff. They identify that the use of passwords requires a user to apply multiple cognitive skills – many of which people with dyslexia struggle to apply due their learning difficulty (2020). Not only are people with dyslexia disadvantaged by passwords, but those with similar cognitive issues such as dyspraxia, ADHD and visual impairments are affected. To get around this issue of passwords being inaccessible password managers such as Dashlane or LastPass can be used, however they require a master password – which if forgotten, locks the user out of the account.

RFID cards which represent the something you **have** factor could be implemented, they are typically used in offices to prevent non-employees accessing areas they do not and should not have access to. A study looking into an RFID smart card found it was a viable authentication method on its own, but that it was more effective as part of a two-factor authentication method with passwords (Hasson et al., 2021). The study however did not consider the possibility of an RFID card being unavailable to

the user (lost or damaged) or being spoofed by an attacker. Another form of two-factor authentication that may be more suitable would be an authentication app, such as Microsoft's Authenticator app. The app is connected to the employee's account and instead of requiring a user to type in a six-digit number in a very small timeframe, a push notification is sent to the employee's device. This push notification can be pressed, where the employee can use face-id, fingerprint, or a pin to sign into the authenticator. The user will then press a button to say that they are trying to access a service or to click the number on the screen (Microsoft Support, 2022). Push notifications are considered to be much more accessible than typical authenticators' process of asking the user to access the app, find the six-digit number to enter and type it in before it refreshes. (Jumpcloud, 2021)

4. Authentication Recommendations

Taking inspiration from the research by Renuad, Johnson and Ophoff, an authentication measure will be designed that is more accessible for every employee – regardless of cognitive abilities. Employees should have a company mobile phone, which will be used to install the 'Microsoft Authenticator' app that provides the *'something you **have'*** aspect. This will ensure that the company has a layer of protection against attackers trying to use stolen credentials. The '*something you **know'*** aspect of the authentication will be a set of images that are randomly generated, apart from one that the user has chosen. Even if an attacker was to correctly guess the image a user has chosen as their 'photo pass', they would still need to use the Authenticator to access the account.

By using a 'photo pass', the user does not need to remember any long passwords – especially if password policies implement an alphanumerical and symbol policy. The user simply needs to click on their photo, meaning that they only need to remember an image. If in the event an employee has a visual impairment and struggles to see, an 'audio pass' can be used instead. The audio pass would be a noise that is distinct for the user to identify when listening to other noises. The wireframes below demonstrate how this would work.

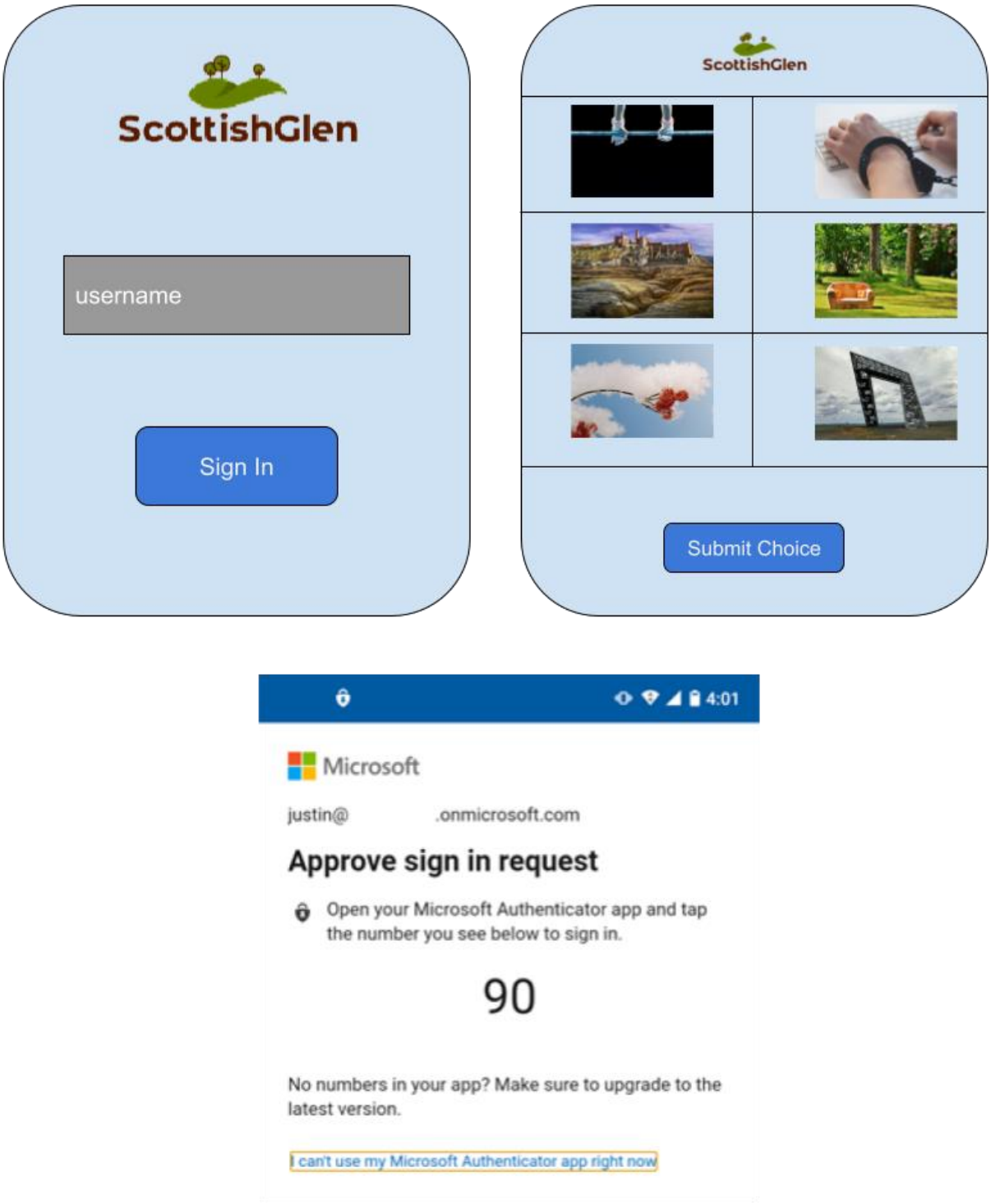

Figure 1 - Wireframes showing how user would sign-in with photo pass authentication

As there are currently no authentication measures in place for the internal web applications, these recommendations should be applied as soon as possible. The authenticator measure should be applied as soon as possible, with a generic username and password mechanism, whilst the pass photo authentication is developed.

References

Alabdan, R., 2020. Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, 12(10), p.168.

Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I., 2021. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 3.

Dashlane Blog. 2022. *How to Run an Effective Phishing Test at Work*. [online] Available at: <https://blog.dashlane.com/phishing-test/> [Accessed 24 May 2022].

Desolda, G., Ferro, L., Marrella, A., Catarci, T. and Costabile, M., 2022. Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys*, 54(8), pp.1-35.

Georgiadou, A., Mouzakitis, S. and Askounis, D., 2021. Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*,.

GOV.UK. 2022. *Cyber Security Breaches Survey 2021*. [online] Available at: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021> [Accessed 18 May 2022].

Hadlington, L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), p.e00346.

Hasson, M., Yassin, A., Yassin, A., Rashid, A., Yaseen, A. and Alasadi, H., 2021. Password authentication scheme based on smart card and QR code. *Indonesian Journal of Electrical Engineering and Computer Science*, 23(1), p.140.

Jampen, D., Gür, G., Sutter, T. *et al.* Don't click: towards an effective anti-phishing training. A comparative literature review. *Hum. Cent. Comput. Inf. Sci.* **10,** 33 (2020). https://doi.org/10.1186/s13673-020-00237-7

JumpCloud. 2022. *Evaluating the Accessibility of Different MFA Factors - JumpCloud*. [online] Available at: <https://jumpcloud.com/blog/evaluating-the-accessibility-of-different-mfa-factors> [Accessed 24 May 2022].

Lal, N.A., Prasad, S. and Farik, M., 2016. A review of authentication methods. *vol*, *5*, pp.246-249.

Microsoft 365. 2022. *Anti-phishing protection - Office 365*. [online] Available at: <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection?view=o365-worldwide> [Accessed 24 May 2022].

NCSC. 2018. *Phishing attacks: defending your organisation.* [online] Available at: <https://www.ncsc.gov.uk/guidance/phishing> [Accessed 24 May 2022].

Rui, Z. and Yan, Z., 2019. A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. *IEEE Access*, 7, pp.5994-6009.

Sharma, T. and Bashir, M., 2020. An Analysis of Phishing Emails and How the Human Vulnerabilities are Exploited. *Advances in Intelligent Systems and Computing*, pp.49-55.

Support.microsoft.com. 2022. *Sign in to your accounts using the Microsoft Authenticator app*. [online] Available at: <https://support.microsoft.com/en-us/account-billing/sign-in-to-your-

accounts-using-the-microsoft-authenticator-app-582bdc07-4566-4c97-a7aa-56058122714c> [Accessed 24 May 2022].

Wen, Z., Lin, Z., Chen, R. and Andersen, E., 2019. What.Hack. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*,.

Zakaria, N.H., Zainul, M.F., Katuk, N., Tahir, H.M. and Omar, M.N., 2018. An evaluation of page token in OpenID Single Sign on (SSO) to thwart phishing attack. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *10*(1-11), pp.19-23.